Datasäkerhet - Lab 2

Course DT523A

Alberto Giaretta, PhD
Centre for Applied Autonomous Sensor Systems (AASS)
Örebro University, Sweden

2022/2023

Packet Sniffing

- Attacker can sniff other recipients' packets in the same network
  - Ethernet cards in promiscuous mode
  - Wireless cards in monitor mode
- Today, you will just analyse your own traffic
  - First with http://seclab1.aga.mpi.aass.oru.se
  - Then with https://seclab2.aga.mpi.aass.oru.se

Report

- Discuss HTTP vs HTTPS results
  - Attach some screenshots that show what you have done
  - What is the lesson?
- Strict deadline for handing in the report
  - ***May 12th 23:59***

Necessary Software

- First of all, install Wireshark
  - https://www.wireshark.org/#download
- For Windows, there is also a portable version
  - Might not work properly though, try it
- For Linux, depends on your distro. E.g., Ubuntu:

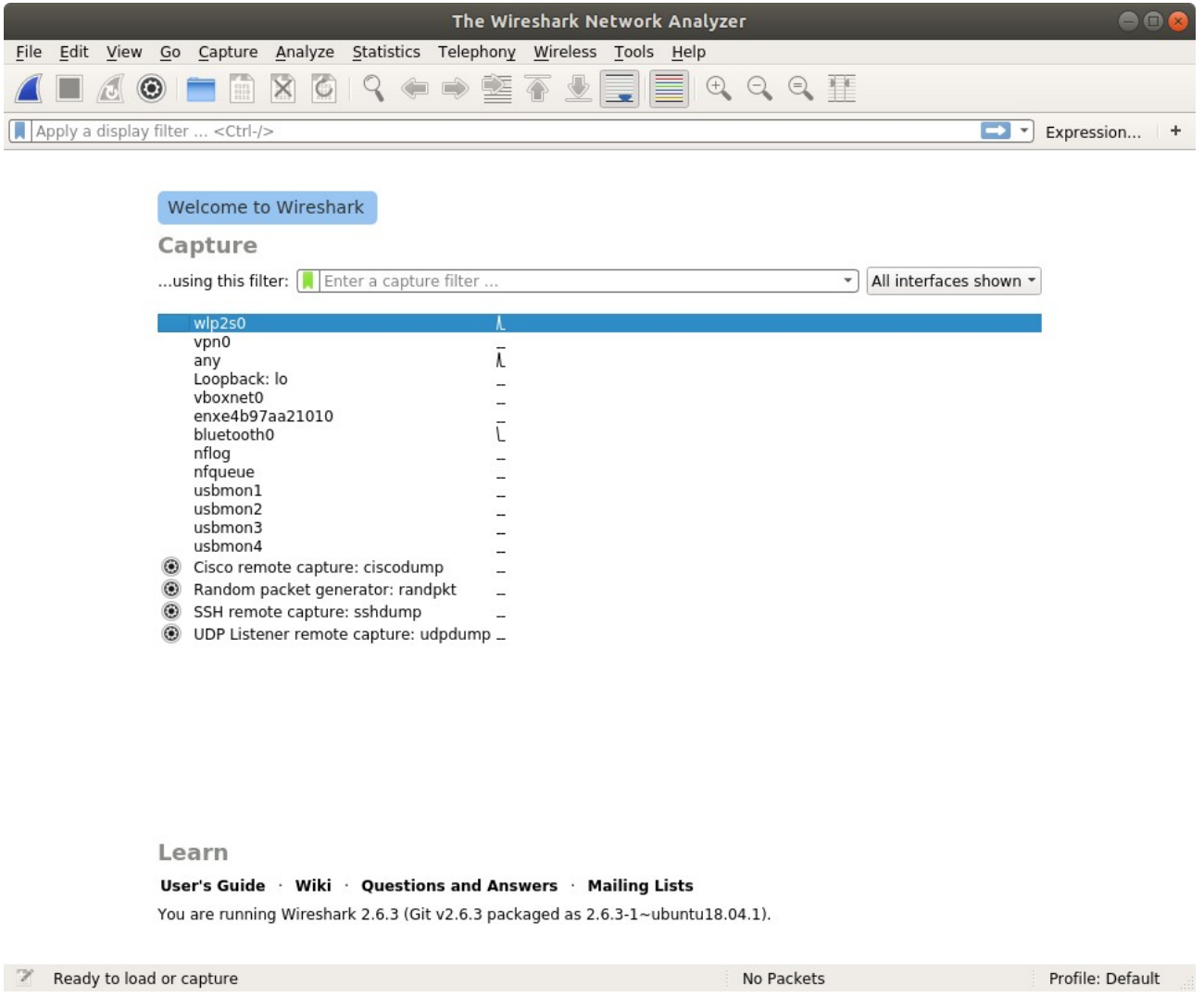
  sudo add-apt-repository ppa:wireshark-dev/stable

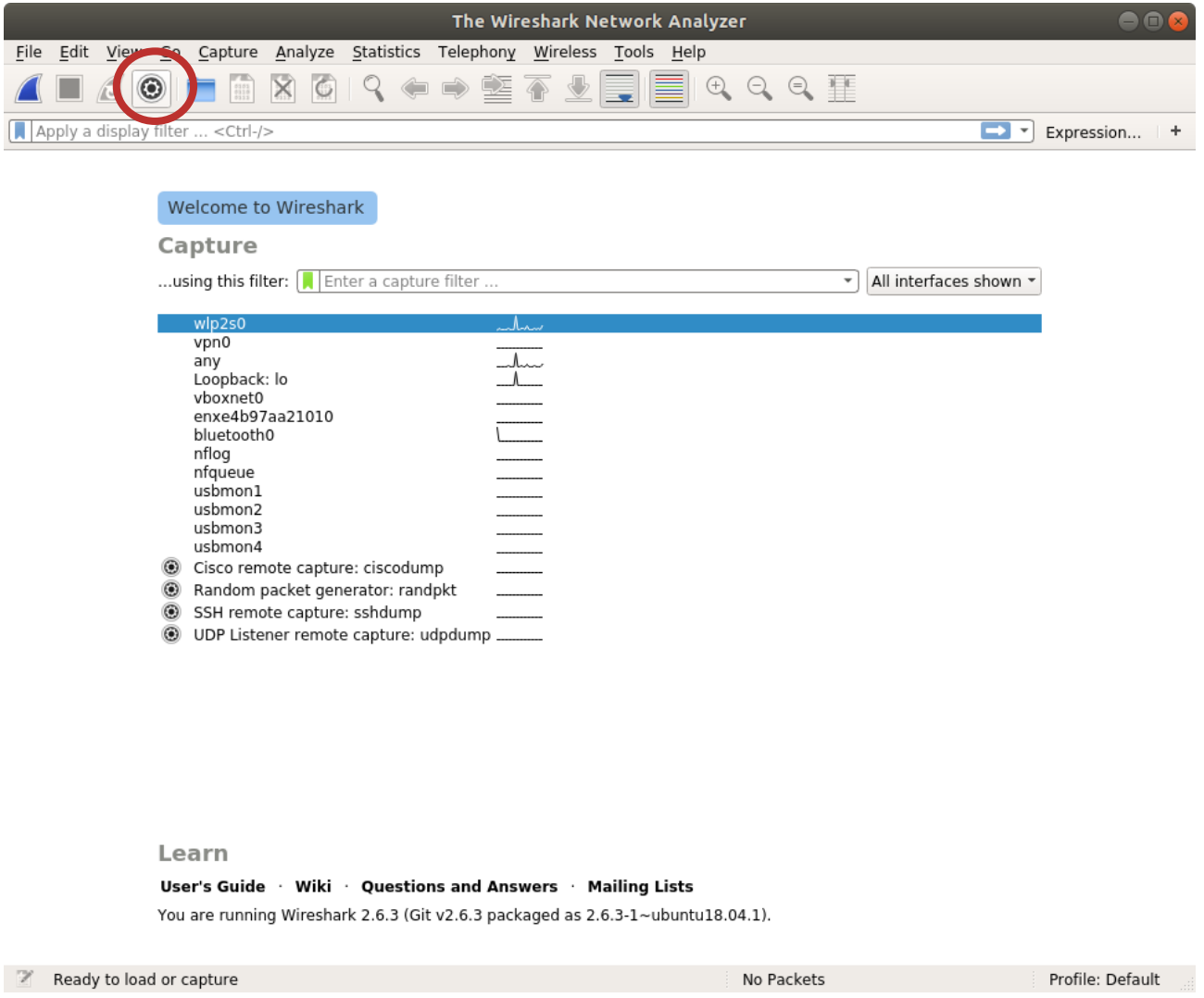
  sudo apt update

  sudo apt install wireshark

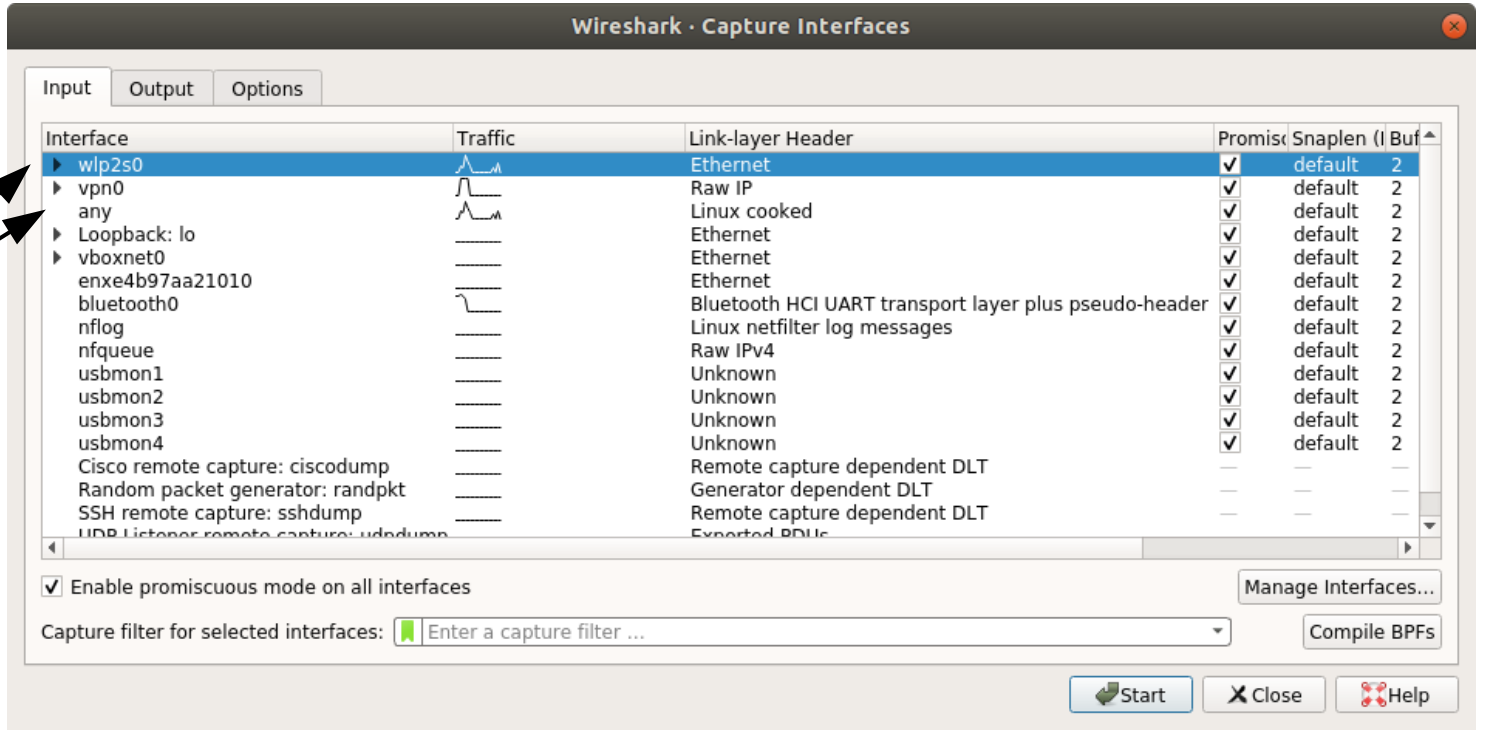
Start Wireshark, and follow the instructions

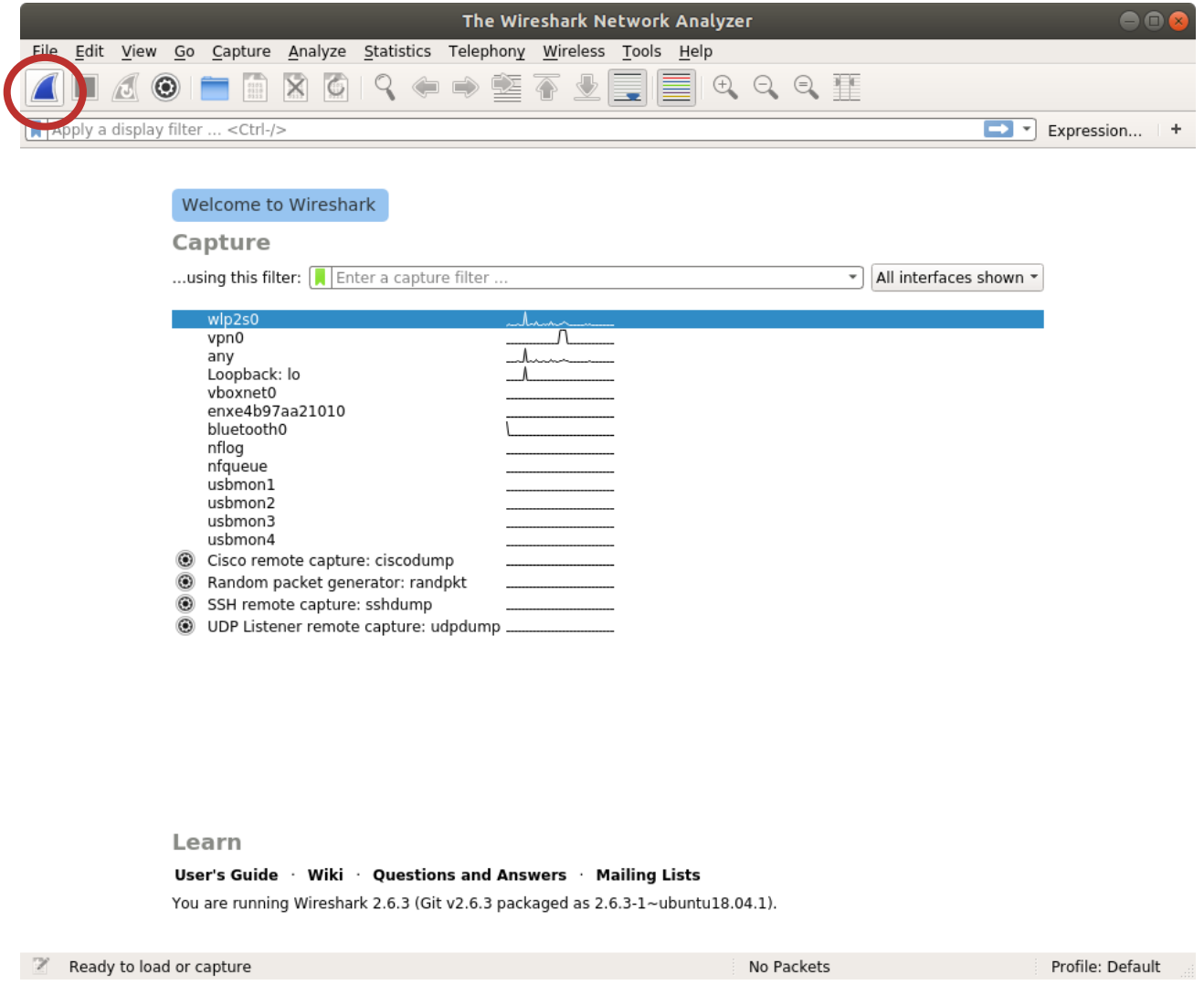
Click the buttons I highlighted in red,
in the following images


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
wlp2s0
vpn0
any
Loopback: lo
vboxnet0
enxe4b97aa21010
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
usbmon3
usbmon4
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.3 (Git v2.6.3 packaged as 2.6.3-1~ubuntu18.04.1).
Ready to load or capture
No Packets
Profile: Default


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
wlp2s0
vpn0
any
Loopback: lo
vboxnet0
enxe4b97aa21010
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
usbmon3
usbmon4
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.3 (Git v2.6.3 packaged as 2.6.3-1~ubuntu18.04.1).
Ready to load or capture
No Packets
Profile: Default

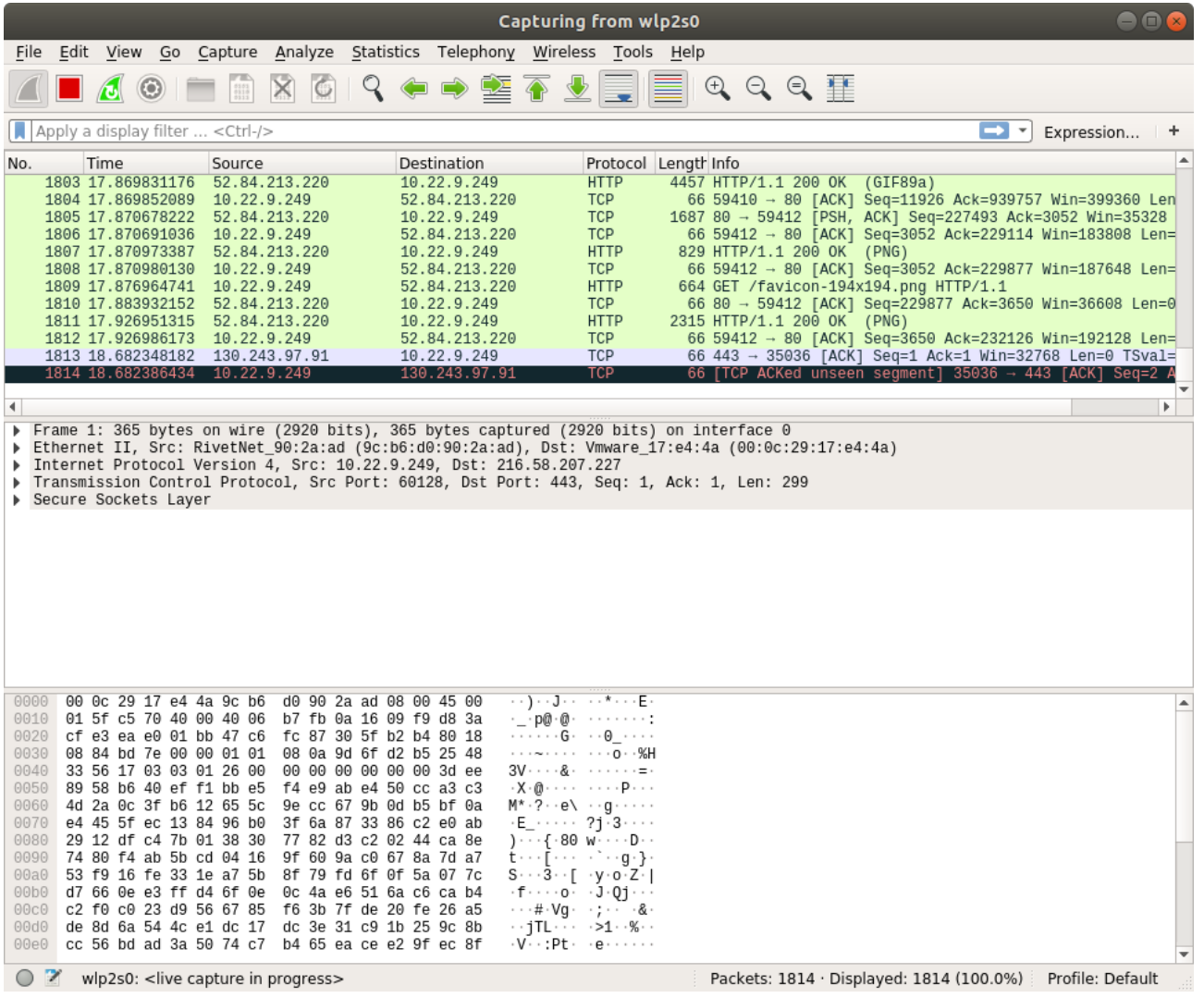
Either select the main ethernet card (name may vary), or the “any” entry

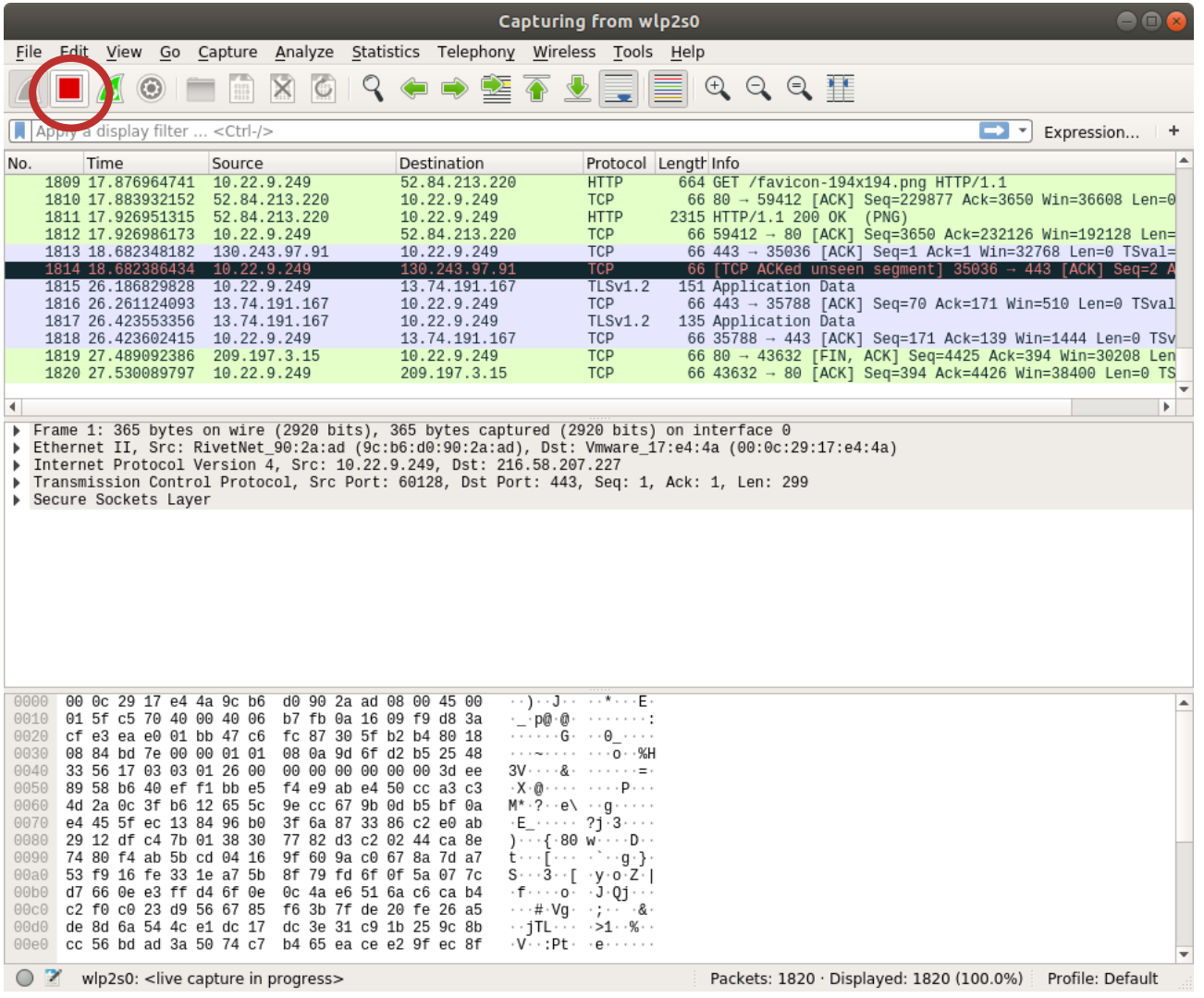


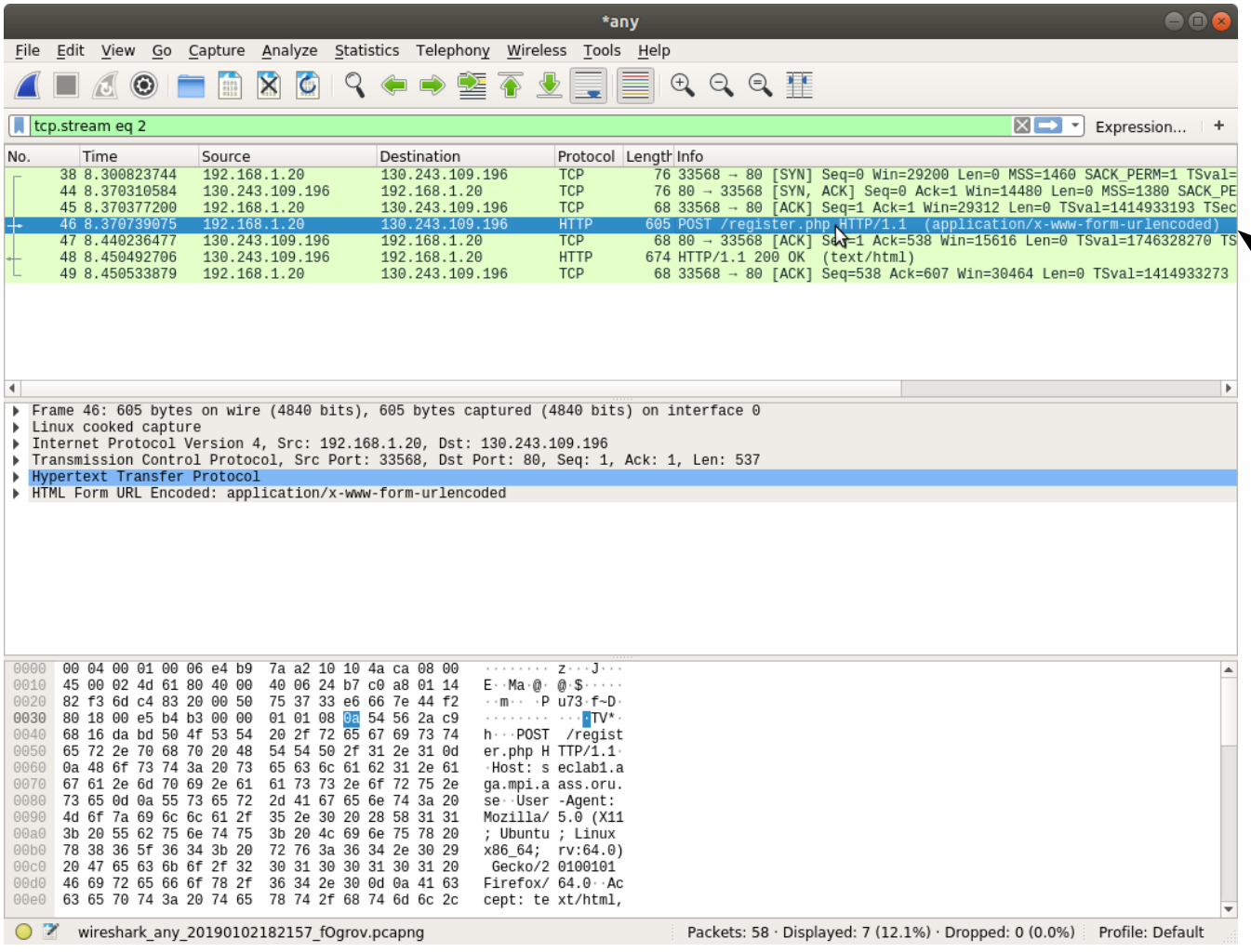

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
wlp2s0
vpn0
any
Loopback: lo
vboxnet0
enxe4b97aa21010
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
usbmon3
usbmon4
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.3 (Git v2.6.3 packaged as 2.6.3-1~ubuntu18.04.1).
Ready to load or capture
No Packets
Profile: Default

Navigate a Webpage

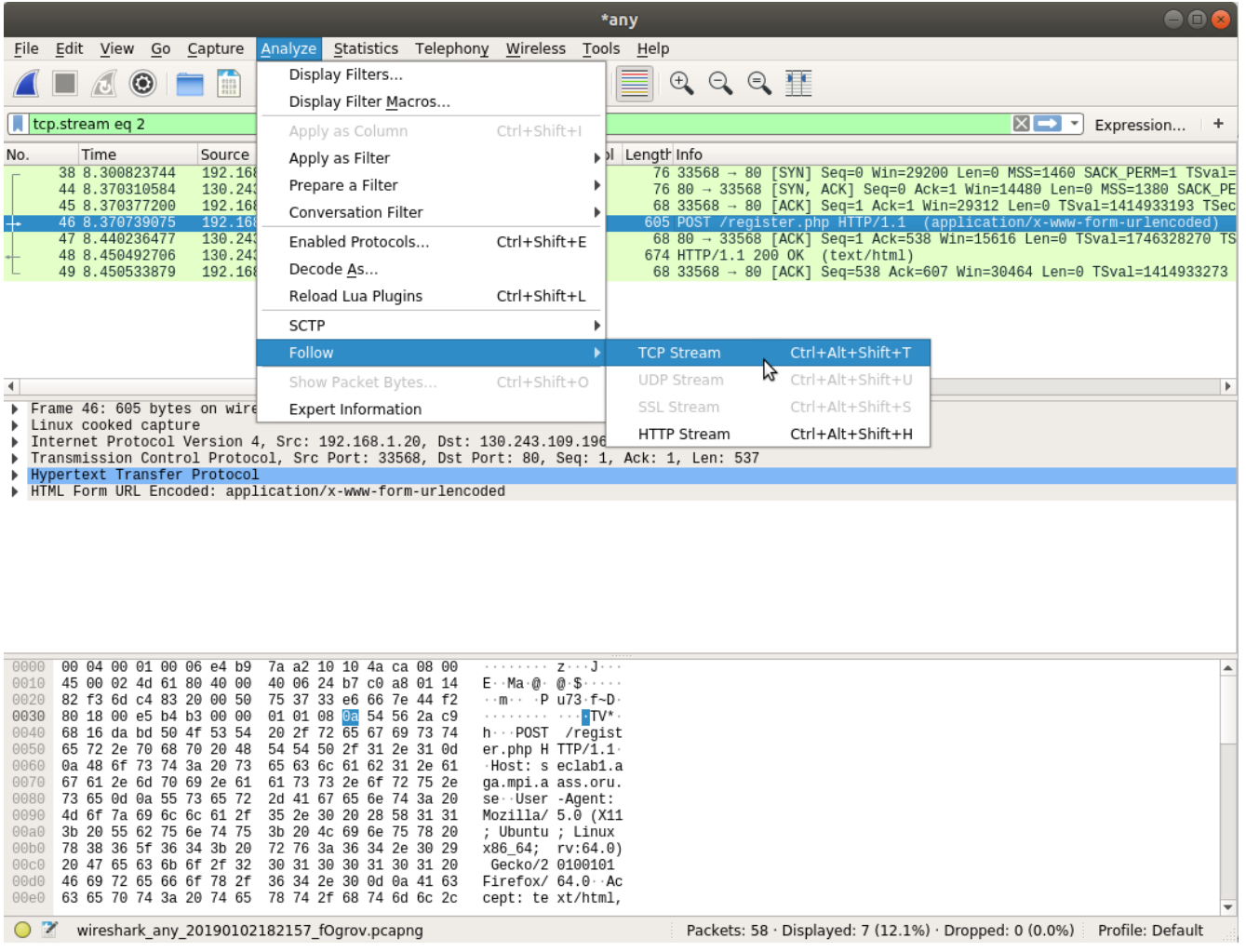
- Leave Wireshark running in the background and open your favourite browser
- Visit http://seclab1.aga.mpi.aass.oru.se
- Insert a username and a password
  - Anything will do, it’s not a real login page
- Press “Login”
- Now go back to Wireshark


Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1803 17.869831176 52.84.213.220 10.22.9.249 HTTP 4457 HTTP/1.1 200 OK (GIF89a)
1804 17.869852089 10.22.9.249 52.84.213.220 TCP 66 59410 → 80 [ACK] Seq=11926 Ack=939757 Win=399360 Len
1805 17.870678222 52.84.213.220 10.22.9.249 TCP 1687 80 → 59412 [PSH, ACK] Seq=227493 Ack=3052 Win=35328
1806 17.870691036 10.22.9.249 52.84.213.220 TCP 66 59412 → 80 [ACK] Seq=3052 Ack=229114 Win=183808 Len=
1807 17.870973387 52.84.213.220 10.22.9.249 HTTP 829 HTTP/1.1 200 OK (PNG)
1808 17.870980130 10.22.9.249 52.84.213.220 TCP 66 59412 → 80 [ACK] Seq=3052 Ack=229877 Win=187648 Len=
1809 17.876964741 10.22.9.249 52.84.213.220 HTTP 664 GET /favicon-194x194.png HTTP/1.1
1810 17.883932152 52.84.213.220 10.22.9.249 TCP 66 80 → 59412 [ACK] Seq=229877 Ack=3650 Win=36608 Len=0
1811 17.926951315 52.84.213.220 10.22.9.249 HTTP 2315 HTTP/1.1 200 OK (PNG)
1812 17.926986173 10.22.9.249 52.84.213.220 TCP 66 59412 → 80 [ACK] Seq=3650 Ack=232126 Win=192128 Len=
1813 18.682348182 130.243.97.91 10.22.9.249 TCP 66 443 → 35036 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=
1814 18.682386434 10.22.9.249 130.243.97.91 TCP 66 [TCP ACKed unseen segment] 35036 → 443 [ACK] Seq=2 A
Frame 1: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) on interface 0
Ethernet II, Src: RivetNet_90:2a:ad (9c:b6:d0:90:2a:ad), Dst: Vmware_17:e4:4a (00:0c:29:17:e4:4a)
Internet Protocol Version 4, Src: 10.22.9.249, Dst: 216.58.207.227
Transmission Control Protocol, Src Port: 60128, Dst Port: 443, Seq: 1, Ack: 1, Len: 299
Secure Sockets Layer
0000 00 0c 29 17 e4 4a 9c b6 d0 90 2a ad 08 00 45 00
0010 01 5f c5 70 40 00 40 06 b7 fb 0a 16 09 f9 d8 3a
0020 cf e3 ea e0 01 bb 47 c6 fc 87 30 5f b2 b4 80 18
0030 08 84 bd 7e 00 00 01 01 08 0a 9d 6f d2 b5 25 48
0040 33 56 17 03 03 01 26 00 00 00 00 00 00 3d ee
0050 89 58 b6 40 ef f1 bb e5 f4 e9 ab e4 50 cc a3 c3
0060 4d 2a 0c 3f b6 12 65 5c 9e cc 67 9b 0d b5 bf 0a
0070 e4 45 5f ec 13 84 96 b0 3f 6a 87 33 86 c2 e0 ab
0080 29 12 df c4 7b 01 38 30 77 82 d3 c2 02 44 ca 8e
0090 74 80 f4 ab 5b cd 04 16 9f 60 9a c0 67 8a 7d a7
00a0 53 f9 16 fe 33 1e a7 5b 8f 79 fd 6f 0f 5a 07 7c
00b0 d7 66 0e e3 ff d4 6f 0e 0c 4a e6 51 6a c6 ca b4
00c0 c2 f0 c0 23 d9 56 67 85 f6 3b 7f de 20 fe 26 a5
00d0 de 8d 6a 54 4c e1 dc 17 dc 3e 31 c9 1b 25 9c 8b
00e0 cc 56 bd ad 3a 50 74 c7 b4 65 ea ce e2 9f ec 8f
wlp2s0: <live capture in progress>
Packets: 1814 · Displayed: 1814 (100.0%)
Profile: Default


Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1809 17.876964741 10.22.9.249 52.84.213.220 HTTP 664 GET /favicon-194x194.png HTTP/1.1
1810 17.883932152 52.84.213.220 10.22.9.249 TCP 66 80 → 59412 [ACK] Seq=229877 Ack=3650 Win=36608 Len=0
1811 17.926951315 52.84.213.220 10.22.9.249 HTTP 2315 HTTP/1.1 200 OK (PNG)
1812 17.926986173 10.22.9.249 52.84.213.220 TCP 66 59412 → 80 [ACK] Seq=3650 Ack=232126 Win=192128 Len=
1813 18.682348182 130.243.97.91 10.22.9.249 TCP 66 443 → 35036 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=
1814 18.682386434 10.22.9.249 130.243.97.91 TCP 66 [TCP ACKed unseen segment] 35036 → 443 [ACK] Seq=2 A
1815 26.186829828 10.22.9.249 13.74.191.167 TLSv1.2 151 Application Data
1816 26.261124093 13.74.191.167 10.22.9.249 TCP 66 443 → 35788 [ACK] Seq=70 Ack=171 Win=510 Len=0 TSval
1817 26.423553356 13.74.191.167 10.22.9.249 TLSv1.2 135 Application Data
1818 26.423602415 10.22.9.249 13.74.191.167 TCP 66 35788 → 443 [ACK] Seq=171 Ack=139 Win=1444 Len=0 TSv
1819 27.489092386 209.197.3.15 10.22.9.249 TCP 66 80 → 43632 [FIN, ACK] Seq=4425 Ack=394 Win=30208 Len
1820 27.530089797 10.22.9.249 209.197.3.15 TCP 66 43632 → 80 [ACK] Seq=394 Ack=4426 Win=38400 Len=0 TS
Frame 1: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) on interface 0
Ethernet II, Src: RivetNet_90:2a:ad (9c:b6:d0:90:2a:ad), Dst: Vmware_17:e4:4a (00:0c:29:17:e4:4a)
Internet Protocol Version 4, Src: 10.22.9.249, Dst: 216.58.207.227
Transmission Control Protocol, Src Port: 60128, Dst Port: 443, Seq: 1, Ack: 1, Len: 299
Secure Sockets Layer
0000 00 0c 29 17 e4 4a 9c b6 d0 90 2a ad 08 00 45 00
0010 01 5f c5 70 40 00 40 06 b7 fb 0a 16 09 f9 d8 3a
0020 cf e3 ea e0 01 bb 47 c6 fc 87 30 5f b2 b4 80 18
0030 08 84 bd 7e 00 00 01 01 08 0a 9d 6f d2 b5 25 48
0040 33 56 17 03 03 01 26 00 00 00 00 00 00 3d ee
0050 89 58 b6 40 ef f1 bb e5 f4 e9 ab e4 50 cc a3 c3
0060 4d 2a 0c 3f b6 12 65 5c 9e cc 67 9b 0d b5 bf 0a
0070 e4 45 5f ec 13 84 96 b0 3f 6a 87 33 86 c2 e0 ab
0080 29 12 df c4 7b 01 38 30 77 82 d3 c2 02 44 ca 8e
0090 74 80 f4 ab 5b cd 04 16 9f 60 9a c0 67 8a 7d a7
00a0 53 f9 16 fe 33 1e a7 5b 8f 79 fd 6f 0f 5a 07 7c
00b0 d7 66 0e e3 ff d4 6f 0e 0c 4a e6 51 6a c6 ca b4
00c0 c2 f0 c0 23 d9 56 67 85 f6 3b 7f de 20 fe 26 a5
00d0 de 8d 6a 54 4c e1 dc 17 dc 3e 31 c9 1b 25 9c 8b
00e0 cc 56 bd ad 3a 50 74 c7 b4 65 ea ce e2 9f ec 8f
wlp2s0: <live capture in progress>
Packets: 1820 · Displayed: 1820 (100.0%)
Profile: Default



Select the “register.php” entry line, or other HTTP streams, to look at the exchanged packets


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Display Filters...
Display Filter Macros...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As...
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes... Ctrl+Shift+O
Expert Information
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
SSL Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
tcp.stream eq 2
Expression...
No. Time Source Length Info
38 8.300823744 192.168 76 33568 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=
44 8.370310584 130.243 76 80 → 33568 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1380 SACK_PE
45 8.370377200 192.168 68 33568 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1414933193 TSec
46 8.370739075 192.168 605 POST /register.php HTTP/1.1 (application/x-www-form-urlencoded)
47 8.440236477 130.243 68 80 → 33568 [ACK] Seq=1 Ack=538 Win=15616 Len=0 TSval=1746328270 TS
48 8.450492706 130.243 674 HTTP/1.1 200 OK (text/html)
49 8.450533879 192.168 68 33568 → 80 [ACK] Seq=538 Ack=607 Win=30464 Len=0 TSval=1414933273
Frame 46: 605 bytes on wire
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 130.243.109.196
Transmission Control Protocol, Src Port: 33568, Dst Port: 80, Seq: 1, Ack: 1, Len: 537
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
0000 00 04 00 01 00 06 e4 b9 7a a2 10 10 4a ca 08 00 .... z...J...
0010 45 00 02 4d 61 80 40 00 40 06 24 b7 c0 a8 01 14 E..Ma.@. @.$.....
0020 82 f3 6d c4 83 20 00 50 75 37 33 e6 66 7e 44 f2 ..m.. .P u73.f~D.
0030 80 18 00 e5 b4 b3 00 00 01 01 08 0a 54 56 2a c9 ....TV*.
0040 68 16 da bd 50 4f 53 54 20 2f 72 65 67 69 73 74 h...POST /regist
0050 65 72 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d er.php H TTP/1.1.
0060 0a 48 6f 73 74 3a 20 73 65 63 6c 61 62 31 2e 61 .Host: s eclab1.a
0070 67 61 2e 6d 70 69 2e 61 61 73 73 2e 6f 72 75 2e ga.mpi.a ass.oru.
0080 73 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 se..User -Agent:
0090 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 Mozilla/ 5.0 (X11
00a0 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 ; Ubuntu ; Linux
00b0 78 38 36 5f 36 34 3b 20 72 76 3a 36 34 2e 30 29 x86_64; rv:64.0)
00c0 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 Gecko/2 0100101
00d0 46 69 72 65 66 6f 78 2f 36 34 2e 30 0d 0a 41 63 Firefox/ 64.0..Ac
00e0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: te xt/html,
wireshark_any_20190102182157_fOgrov.pcapng
Packets: 58 · Displayed: 7 (12.1%) · Dropped: 0 (0.0%)
Profile: Default

Can you see anything interesting?

Navigate another Webpage

- Repeat the aforementioned steps
- This time use the webpage https://seclab2.aga.mpi.aass.oru.se
  - The difference is that this link has “https://”
- What’s the difference between HTTP and HTTPS?